PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-107084
(43)Date of publication of application : 21.04.1995

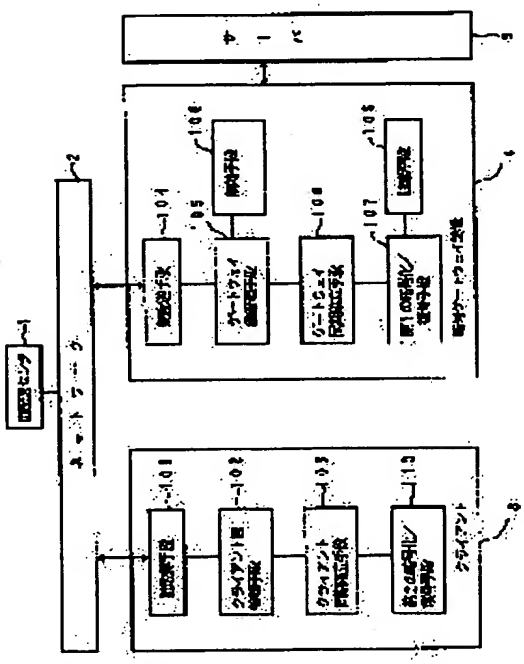
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/28

(21)Application number : 05-250852
(22)Date of filing : 06.10.1993

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : YAMAGUCHI TOSHIKAZU

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To provide a cipher communication system capable of performing cipher communication without influencing existing hardwares and application.
CONSTITUTION: A cipher gateway device 4 connected to a server 5 as a front- end processor establishes a session for communication between a client and the server with the detection of a cipher communication request from the client 3 as a trigger. At the time, with the detection of the cipher communication request from the client 3 as the trigger, the cipher gateway device 4 obtains a session key front a key delivery center 1, delivers it to the client 3 and shares the same session key between the client and the gateway device.



LEGAL STATUS

[Date of request for examination]	23.10.1998
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3263879
[Date of registration]	28.12.2001
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁(JP)　(12)特許公報（Ｂ２）　(11)特許番号

特許第３２６３８７９号
（Ｐ３２６３８７９）

(45)発行日　平成14年3月11日(2002.3.11)　(24)登録日　平成13年12月28日(2001.12.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		
Ｈ０４Ｌ	9/08	Ｈ０４Ｌ	9/00	６０１　Ｂ
	12/28		11/00	３１０　Ｚ

請求項の数３　(全１４頁)

(21)出願番号　特願平5-250852

(22)出願日　平成5年10月6日(1993.10.6)

(65)公開番号　特開平7-107084

(43)公開日　平成7年4月21日(1995.4.21)

審査請求日　平成10年10月23日(1998.10.23)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72)発明者　山口　利和
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

(74)代理人　100070150
弁理士　伊東　忠彦

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】暗号通信システム

1

(57)【特許請求の範囲】

【請求項１】　ネットワークを介して複数のクライアントならびにサーバが鍵配送センタに接続され、該鍵配送センタが生成したセッション鍵を該ネットワークを介して入手することにより、任意のクライアント・サーバ間でセッションを確立して暗号通信を行う通信システムにおいて、

該サーバと該ネットワークの間に位置し、サーバとの通信用セッションの確立時にクライアントが出力する暗号通信要求を検索し、該暗号通信要求を契機としてクライアントとの鍵配送用セッションを確立すると共に、該鍵配送センタからセッション鍵を取得し、該クライアントに配送する鍵配送手段と、取得した該セッション鍵を管理するゲートウェイ鍵管理手段と、該クライアントとの暗号同期を確立するゲートウェイ同期確立手段と、該同

2

期確立手段により同期完了報告後に該ゲートウェイ鍵管理手段より該セッション鍵を取得し、パケットを復号または暗号化する第１の暗号化／復号手段とを含む暗号ゲートウェイ装置と、

該サーバとの通信用セッション確立時に、該暗号ゲートウェイ装置に暗号通信を要求し、セッション鍵を取得する鍵取得手段と、取得した該セッション鍵を管理するクライアント鍵管理手段と、該暗号ゲートウェイ装置との暗号同期を確立するクライアント同期確立手段と、同期確立後、該クライアント鍵管理手段より該セッション鍵を取得し、パケットを復号または暗号化する第２の暗号化／復号手段とを含むクライアントを有し、

該クライアント・サーバ間の通信用セッション確立時に、該暗号ゲートウェイ装置が該クライアントからの暗号通信要求を検出してクライアントと鍵配送用セッショ

ンを確立すると共に、該鍵配送センタから該セッション鍵を取得して、該クライアントに配送することにより、該クライアント・該暗号ゲートウェイ装置間で共通のセッション鍵を共有することを特徴とする暗号通信システム。

【請求項２】　前記暗号ゲートウェイ装置は、前記クライアント・前記サーバ間の通信用セッション切断を検出し、前記ゲートウェイ鍵管理手段に保持する当該セッションのセッション鍵を無効にする無効手段を含む請求項１記載の暗号通信システム。

【請求項３】　前記暗号ゲートウェイ装置は、前記クライアント・前記サーバ間で通信するパケットを受信し、前記クライアントと前記暗号ゲートウェイ装置間で暗号の同期確立が完了していないセッションのパケットを破棄する破棄手段を含む請求項１記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、任意のクライアントとサーバがセッションを確立し、共通鍵暗号アルゴリズムを用いて暗号通信を行う通信システムに係り、特に、ネットワークを介して複数のクライアント並びにサーバが鍵配送センタに接続され、鍵配送センタが生成したセッション鍵をネットワークを介して入手する暗号通信システムに関する。

【０００２】

【従来の技術】図１２は、従来の暗号通信システムの構成を示す。同図に示す従来の暗号通信システムは、ネットワーク２を介して、複数のクライアント3_1～3_3及びサーバ５が鍵配送センタ１に接続され、鍵配送センタ１が生成したセッション鍵をクライアント３またはサーバ５が入手する。

【０００３】図１３は、従来の暗号通信システムを説明するための図である。同図（Ａ）は、鍵配送センタ１にセッション鍵を要求する場合に、クライアント３からアプリケーションプログラムを用いて要求する場合を示し、同図（Ｂ）は、サーバ５からアプリケーションプログラムを用いて要求する場合を示す。このように、クライアント３またはサーバ５がアプリケーションプログラムを用いて通信に使用するセッション鍵を取得する。このセッション鍵をクライアント３とサーバ５間で共有し、以降の通信パケットをこのセッション鍵を用いて暗号化或いは、復号し、暗号通信を行う。

【０００４】このように、従来の暗号通信システムは、広い地域に分散した事業所等の特定の端末間で暗号通信を行うＬＡＮ等に効果的に利用できるものである。

【０００５】

【発明が解決しようとする課題】しなしながら、上記従来の方式では、暗号通信に先立ち、クライアント或いはサーバ上で走行するアプリケーションプログラムが鍵配送センタとセッションを確立し、鍵配送センタからセッション鍵を取得し、かつ通信相手のサーバ或いはクライアントのアプリケーションに同じセッション鍵を送信する処理が必要となる。

【０００６】一方、コネクション型のネットワークを介して、クライアント・サーバ間で通信を行う通信プログラムの数は膨大であり、これらを暗号通信対応に変更する場合には、個別にアプリケーションプログラムやクライアント或いはサーバのハードウェアを改造する必要があり、改造規模や工数が大きくなり、これに伴って、開発費も大きくなるという問題がある。

【０００７】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、既存のハードウェアやアプリケーションに影響を与えることなく、暗号通信を行うことができる暗号通信システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】図１は、本発明の原理構成図である。本発明は、ネットワーク２を介して複数のクライアント３ならびにサーバ５が鍵配送センタ１に接続され、鍵配送センタ１が生成したセッション鍵をネットワーク２を介して入手することにより、任意のクライアント３・サーバ５間でセッションを確立して暗号通信を行う通信システムにおいて、サーバ５とネットワーク２の間に位置し、サーバ５との通信用セッションの確立時にクライアント３が出力する暗号通信要求を検索し、暗号通信要求を契機としてクライアント３との鍵配送用セッションを確立すると共に、鍵配送センタ１からセッション鍵を取得し、クライアント３に配送する鍵配送手段１０４と、取得したセッション鍵を管理するゲートウェイ鍵管理手段１０５と、クライアント３との暗号同期を確立するゲートウェイ同期確立手段１０６と、同期確立手段１０６により同期完了報告後にゲートウェイ鍵管理手段１０５よりセッション鍵を取得し、パケットを復号または暗号化する第１の暗号化／復号手段１０７とを含む暗号ゲートウェイ装置４と、サーバ５との通信用セッション確立時に、暗号ゲートウェイ装置４に暗号通信を要求し、セッション鍵を取得する鍵取得手段１０１と、取得したセッション鍵を管理するクライアント鍵管理手段１０２と、暗号ゲートウェイ装置との暗号同期を確立するクライアント同期確立手段１０３と、同期確立後、クライアント鍵管理手段１０２よりセッション鍵を取得し、パケットを復号または暗号化する第２の暗号化／復号手段１１０とを含むクライアント３を有し、クライアント・サーバ５間の通信用セッション確立時に、暗号ゲートウェイ装置がクライアント３からの暗号通信要求を検出してクライアント３と鍵配送用セッションを確立すると共に、鍵配送センタ１からセッション鍵を取得して、クライアント３に配送することにより、クライアント・暗号ゲートウェイ装置間で共通のセッション鍵を

共有する。

【０００９】また、本発明の暗号ゲートウェイ装置４は、クライアント３・サーバ５間の通信用セッション切断を検出し、ゲートウェイ鍵管理手段１０５に保持する当該セッションのセッション鍵を無効にする無効手段１０８を含む。

【００１０】また、本発明の暗号ゲートウェイ装置４は、クライアント３・サーバ５間で通信するパケットを受信し、クライアント３と暗号ゲートウェイ装置４間で暗号の同期確立が完了していないセッションのパケットを破棄する破棄手段１０９を含む。

【００１１】

【作用】図２は、本発明の通信シーケンスの概要を示す。本発明は、サーバにフロントエンドプロセッサとして、暗号ゲートウェイ装置を接続し、この暗号ゲートウェイ装置がクライアントからの暗号通信要求の検出（ステップ１）を契機としてクライアント・サーバ間の通信用セッションを確立する（ステップ２）。このとき、暗号ゲートウェイ装置がクライアントからの暗号通信要求の検出を契機として、鍵配送センタからセッション鍵を取得（ステップ３）して、クライアントに配送する（ステップ４）ことにより、クライアント・ゲートウェイ装置間で同一のセッション鍵を共有する（ステップ５）。クライアントは暗号ゲートウェイ装置との暗号同期を確立し、これ以降、クライアント・サーバ間のセッションが切断されるまでクライアント・暗号ゲートウェイ装置間の暗号通信が可能となる（ステップ６）。

【００１２】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【００１３】図３は、本発明のシステム全体図である。同図に示す通信システムは、ネットワーク２を介して接続される鍵配送センタ１、クライアント３、暗号ゲートウェイ装置４、暗号ゲートウェイ装置４に接続されるサーバ５により構成される。同図において、サーバ５の前段に暗号ゲートウェイ装置４が接続されているが、クライアント３の前段に暗号ゲートウェイ装置４を接続することも考えられる。本実施例では、暗号ゲートウェイ装置４はサーバ５のフロントエンドとして接続されており、簡単のため、暗号ゲートウェイ装置４には１つのサーバ５が接続されるものとして説明する。

【００１４】鍵配送センタ１は、セッション鍵を生成して暗号ゲートウェイ装置４に送信する。ネットワーク２は、クライアント３－サーバ５間、鍵配送センタ１－暗号ゲートウェイ装置４間、クライアント３－暗号ゲートウェイ装置４間でセッションを確立し、通信を行う。暗号化ゲートウェイ装置４は、クライアント３－サーバ間５でやり取りするパケットを暗号化／復号する。

【００１５】図４は、本発明の一実施例のシステム構成図である。同図中、図３と同一構成部分には同一符号を

付す。同図に示すクライアント３は、セッション制御部３１、セッション鍵配送部３２、鍵管理部３３、暗号同期確立部３４、暗号化／復号部３５、送信／受信部３６から構成される。

【００１６】セッション制御部３１は、サーバ５との通信用セッション確立時に、プロトコルに暗号通信要求のメッセージを挿入し、暗号ゲートウェイ装置４に暗号通信要求を行う。セッション鍵配送部３２は、暗号ゲートウェイ装置４と鍵配送用セッションを確立し、暗号ゲートウェイ装置４からセッション鍵を取得し、鍵管理部３３に配送する。

【００１７】鍵管理部３３は、セッション鍵配送部３２から受け取ったセッション鍵をセッション毎に管理する。暗号同期確立部３４は、クライアント３と暗号ゲートウェイ装置４間でセッション鍵配送部３２によるセッション確立を契機に暗号通信の同期を確立する。

【００１８】暗号化／復号部３５は、アプリケーションから受け取ったデータを、鍵管理部３３が保持する当該セッション鍵を使用して暗号化、または、サーバ５から受け取った暗号化されたパケットを復号する。送信／受信部３６は、ネットワーク２から（へ）暗号化されたパケットを受信（送信）する。

【００１９】暗号ゲートウェイ装置４は、セッション確立／切断のモニタ部４１、セッション鍵配送部４２、鍵管理部４３、暗号同期確立部４４、暗号化／復号部４７、送信／受信部４５、及びセッション識別部４６より構成される。

【００２０】セッション確立／切断のモニタ部４１は、クライアント３とサーバ５間で通信するパケットをモニタし、セッションの確立用パケットであり、かつヘッダのオプションに“暗号通信要求”のメッセージが挿入されているパケット及びセッション切断用パケットを検出する。また、クライアント３から暗号通信要求が出されていることをセッション鍵配送部４２に通知する。さらに、セッション切断がある場合には、この旨を鍵管理部４３に通知する。

【００２１】セッション鍵配送部４２は、セッション確立／切断のモニタ部４１から報告される暗号通信要求を契機としてクライアント３との間で鍵配送用セッションを確立し、鍵配送センタ１からセッション鍵を取得し、クライアント３に配送する。また、セッション鍵を鍵管理部４３に配送する。

【００２２】鍵管理部４３は、セッション鍵配送部４２から受け取ったセッション鍵をセッション毎に管理するとともに、セッション確立／切断のモニタ部４１から報告されるセッション切断を契機として当該セッション鍵を無効にする。

【００２３】暗号同期確立部４４は、クライアント３と暗号ゲートウェイ装置４間で暗号通信の同期を確立し、同期完了を暗号化／復号部４７に報告する。

【００２４】送信／受信部４５は、クライアント３或いはサーバ５から（へ）パケットを受信（送信）する。

【００２５】セッション識別部４６は、送信／受信部４５から受け取ったパケットのＩＰヘッダ及びＴＣＰヘッダから送信元ＩＰアドレス、送信元ポート番号、送信先ＩＰアドレス及び送信先ポート番号を取り出し、セッション番号を識別する。

【００２６】暗号化／復号化部４７は、暗号同期確立部４４から同期完了報告前に受信したパケットを破棄し、同期完了報告後のパケットについては、セッション識別部４６から受け取ったセッション番号をキーとして鍵管理部４３からセッション鍵を取得し、サーバ５宛のパケットであれば、当該パケットを復号し、クライアント３宛のパケットであれば、当該パケットを暗号化する。

【００２７】図５は、ＴＣＰ／ＩＰ・ＬＡＮで使用するプロトコルをＯＳＩの参照モデルに準拠して記述している。データリンクレイヤは、ＭＡＣ（Media Access Control）プロトコル、ネットワークレイヤは、ＩＰ（Internet protocol）、トランスポートレイヤはＴＣＰ(Transmit Control Protocol）で実現されており、ＡＰは、ＴＣＰレイヤ間でセッションを確立する。

【００２８】図６は、ＴＣＰ／ＩＰ・ＬＡＮに接続されたクライアント・サーバ間で通信する際に使用するパケット・フォーマットを示す。

【００２９】パケットは、ＭＡＣヘッダ（ＭＡＣ＿Ｈ），ＩＰヘッダ（ＩＰ＿Ｈ）及びＴＣＰヘッダ（ＴＣＰ＿Ｈ）からなるヘッダと、ＡＰデータ及びパケット全体のフレームチェック・シーケンス（ＦＣＳ）から構成される。暗号ゲートウェイ装置４がアプリケーションデータを暗号化／復号することにより、クライアント３と暗号ゲートウェイ装置４間で暗号通信を行う。アプリケーションデータを暗号化することにより、ＩＰルータを介したネットワークを使用して通信を行うことができる。なお、送信側のＩＰアドレス（ＩＰヘッダに規定）及びポート番号（ＴＣＰヘッダに規定）と受信側のＩＰアドレス及びポート番号によりクライアント・サーバ間のセッションが一意に決定される。暗号ゲートウェイ装置４のセッション識別部４６はこのように、パケットの送信側のＴＣＰヘッダ、ＩＰヘッダと受信側のＩＰアドレス及びポート番号によりセッションを識別する。

【００３０】図７は、ＴＣＰヘッダのフォーマットを示す。同図において“＿”は本発明に直接関係しないので、説明は省略する。

【００３１】“ＳＲＣ＿ＰＯＲＴ”及び“ＤＳＴ＿ＰＯＲＴ”は各々発信元のポート番号、送信先のポート番号を示す。“ＣＦ＿ＰＯＲＴ”は、各々送信元のポート番号、送信先のポート番号を示す。“ＣＦ（制御フラグ）は、“ＳＹＮ:Synchronize flag （セッションの確立）”、“ＡＣＫ：Acknowledgement flag（確認）”及び“ＦＩＮ:Fin flag （セッションの切断）”等から構成される。

【００３２】セッションの確立には、“ＳＹＮ”及び“ＡＣＫ”が、切断には“ＦＩＮ”及び“ＡＣＫ”が使用される。

【００３３】図８は、本発明の一実施例のセッション確立手順のシーケンスチャートである。クライアント３からのパケットにセッション確立のフラグ“ＳＹＮ”がサーバ５に渡され（ステップ１０１）、サーバ５が“ＳＹＮ”に対して、“ＡＣＫ”により応答する。この場合、サーバ５は、“ＳＹＮ＋ＡＣＫ”をクラインアト３に渡す（ステップ１０２）。これに対して、クライアント３は、サーバ５に応答の“ＡＣＫ”を通知する（ステップ１０３）。これにより、クライアント３とサーバ５間のセッションが確立する（ステップ１０４）。

【００３４】図９は、本発明の一実施例のセッション切断手順のシーケンスチャートを示す。クライアント３からパケットにセッションの切断のフラグ“ＦＩＮ”がサーバ５に渡されると（ステップ２０１）、サーバ５は、“ＡＣＫ”により応答すると共に（ステップ２０２）、セッションの切断のための“ＦＩＮ”をクライアント３に通知する（ステップ２０３）。クライアント３はサーバからの通知を受け取った旨をサーバに“ＡＣＫ”により通知する（ステップ２０４）。これにより、クライアント・サーバ間のセッションが切断される（ステップ２０５）。

【００３５】なお、セッションの確立／切断手順の詳細は、“上原「異機種接続とＬＡＮ絵とき読本、ｐｐ．１３７～１４１、オーム社」”を参照されたい。

【００３６】クライアント３から暗号ゲートウェイ装置４に対する暗号通信要求には、ＴＣＰ或いは、ＩＰヘッダのオプションを利用して、メッセージ（暗号通信要求）送信する方法を利用できる。

【００３７】図１０は、本発明の一実施例の鍵配送手順を示すシーケンスチャートである。なお、クライアント３及び暗号ゲートウェイ装置４の暗号鍵K_{c1}及びK_{gw}は、各装置のインストール時に内部の保持しており、外部から見ることはできない。

【００３８】同図中、$K_S = dK_{c1}(C_{c1})$：K_Sは暗号文C_{c1}を暗号鍵K_{c1}で復号した結果である。

【００３９】（手順１）クライアント３は、サーバ５と通信用セッションを確立する。この時、クライアント３のセッション制御部３１は、パケットのＴＣＰヘッダのオプションに“暗号通信要求”メッセージを挿入する（ステップ３０１）。

【００４０】（手順２）暗号ゲートウェイ装置４のセッション確立／切断のモニタ部４１は、クライアント・サーバ間で通信するパケットをモニタし（ステップ３０２）、セッション鍵配送部４２において、セッション確立用でかつ“暗号通信要求”が挿入されたパケットを検出した場合に、クライアント３と鍵配送用セッションを

確立する（ステップ３０３）。

【００４１】（手順３）クライアント３は、暗号ゲートウェイ装置４にクライアント３の識別子ID_{c1}を送信する（ステップ３０４）。

【００４２】（手順４）暗号ゲートウェイ装置４は、鍵配送センタ１にアクセスし、鍵取得手順（ステップ３０５）（詳しくは、図１１において説明する）によりクライアント３及び暗号ゲートウェイ装置４それぞれの暗号鍵（K_{c1}及びK_{gw}）で暗号化されたセッション鍵（C_{c1}及びC_{gw}）を鍵配送センタ１から受信する（ステップ（ステップ３０６）。

【００４３】（手順５）暗号ゲートウェイ装置４の鍵管理部４３は、鍵配送センタ１より受け取ったC_{gw}を暗号ゲートウェイ装置４の暗号鍵K_{gw}で復号し、セッション鍵K_Sを取得する（ステップ３０７）。セッション鍵K_Sは、サーバ５とのセッションを切断するまで保持される。

【００４４】（手順６）暗号ゲートウェイ装置４のセッション鍵配送部４２は、クライアント３に鍵配送センタ１から受信したセッション鍵C_{c1}を配送する（ステップ３０８）。

【００４５】（手順７）クライアント３は、暗号ゲートウェイ装置４からセッション鍵C_{c1}（暗号）を受信する（ステップ３０９）。

【００４６】（手順８）クライアント３は、自分の暗号鍵K_{c1}を用いて暗号ゲートウェイ装置４から配送されたC_{c1}を復号し、セッション鍵K_Sを取得する（ステップ３１０）。

【００４７】（手順９）クライアント３の暗号同期確立部３４と暗号ゲートウェイ装置４の暗号同期確立部４４は、暗号同期の確立を行う（ステップ３１１）。暗号同期の確立が完了すると、クライアント３は暗号ゲートウェイ装置４とのセッションを切断する（ステップ３１２）。なお、暗号同期の確立方法は、本発明の目的とするところではないので、詳細な説明は省略する。

【００４８】（手順１０）以降、共通のセッション鍵K_Sを用いて、クライアント３と暗号ゲートウェイ装置４間の暗号通信が可能となる（ステップ３１３）。

【００４９】（手順１１）暗号ゲートウェイ装置４は、クライアント３からサーバ５宛のパケットを受信し、暗号化／復号部４７でセッション識別部４６により識別された該当するセッション鍵を使用して、パケットを復号する（ステップ３１４）。この復号されたパケット（平文のパケット）をサーバ５に送信することにより、暗号ゲートウェイ装置４とサーバ５間で非暗号通信が可能である（ステップ３１５）。

【００５０】また、サーバ５からクライアント３宛のパケットについては、暗号ゲートウェイ装置４の暗号化／復号部４７にて、パケットを暗号化する。即ち、サーバ５から暗号ゲートウェイ装置４に対して平文を送信し

（ステップ３１３’）、暗号ゲートウェイ装置４の暗号化／復号部４７にて暗号化し（ステップ３１４’）、セッション鍵K_Sを用いて暗号ゲートウェイ装置４とクライアント３間の暗号通信を行う（ステップ３１５’）。

【００５１】図１１は、本発明の一実施例の暗号ゲートウェイ装置の鍵配送センタからの鍵取得のシーケンスチャートである。

【００５２】（手順１）暗号ゲートウェイ装置４は、鍵配送センタ１とセッションを確立する（ステップ４０１）。

【００５３】（手順２）暗号ゲートウェイ装置４は、鍵配送センタ１にクライアント３及び暗号ゲートウェイ装置４の識別子ID_{c1}及びID_{gw}を送信する（ステップ４０２）。なお、識別子ID_{c1}及びID_{gw}は装置を識別するために使用するＩＰアドレス或いは、ＭＡＣアドレスである。

【００５４】（手順３）鍵配送センタ１は、乱数を発生し、セッション鍵K_Sを生成する。さらに、クライアント及び暗号ゲートウェイ装置４の暗号鍵K_{c1}及びK_{gw}を識別子ID_{c1}、ID_{gw}に基づいて検索（或いは生成）する。ここで、K_{c1}及びK_{gw}の検索（或いは生成）する方法は、本発明の直接的な目的ではないので説明を省略する。検索によりK_{c1}及びK_{gw}を取得する場合には、装置の識別子及び暗号鍵を鍵配送センタ１のデータベースに登録する手段が必要であることはいうまでもない。さらに、K_{c1}及びK_{gw}を生成する方法は、“小柳津、田中『ＵＵＩを利用した鍵配送方式、信学技報』、ＯＦＳ９２－３１”を参照されたい。

【００５５】上記に示すK_{c1}及びK_{gw}を用いて、鍵配送センタ１は、K_Sを暗号化し、C_{c1}及びC_{gw}を生成する（ステップ４０３）。

【００５６】（手順４）鍵配送センタ１は、暗号ゲートウェイ装置４にC_{c1}及びC_{gw}を送信する（ステップ４０４）。

【００５７】（手順５）暗号ゲートウェイ装置４は、鍵配送センタとのセッションを切断する（ステップ４０５）。

【００５８】なお、本発明は、上記の実施例に限定されることなく、以下の点でも種々応用が可能である。

【００５９】ここでは、暗号ゲートウェイ装置４と鍵配送センタ１間は、セッションを確立して通信を行う例を説明したが、ＵＤＰプロトコルを使用するコネクションレス型の通信を使用してもよいし、また、他の通信プロトコルを使用してもよいということは、いうまでもない。

【００６０】さらに、本発明は、鍵配送アルゴリズムを特定したものではない。従って、送信するデータの内容（ここでは、ID_{c1}、ID_{gw}，C_{c1}及びC_{gw}）を変更すれば、相手端末の認証ができることはいうまでもない。詳しくは、文献“小柳津、田中『ＵＵＩを利用した鍵配

11

送方式』、信学技報、ＯＦＳ９２－３１”を参照されたい。

【００６１】上記実施例では、暗号ゲートウェイ装置４に１つのサーバが接続されているパターンを説明したが、１つの暗号ゲートウェイ装置４に複数のサーバを接続することも考えられる。また、暗号ゲートウェイ装置４をサーバに接続したが、クライアント側に接続することも考えられる。

【００６２】

【発明の効果】上述のように本発明によれば、暗号暗号ゲートウェイ装置がクライアントからの暗号通信要求を検出し、これを契機としてクライアントと鍵配送セッションを確立すると共に、鍵配送センタにアクセスし、通信に使用するセッション鍵を取得し、通信相手であるクライアントに当該セッション鍵を配送し、クライアントと暗号ゲートウェイ間で共通のセッション鍵を共有し、このセッション鍵を用いて暗号通信を行うため、従来のように、暗号通信対応に既存のアプリケーションやハードウェアを改造する必要がなく、経済化を図ることができる。

【図面の簡単な説明】

【図１】本発明の原理構成図である。

【図２】本発明の概要のシーケンスである。

【図３】本発明のシステム全体図である。

【図４】本発明の一実施例のシステム構成図である。

【図５】ＴＣＰ／ＩＰ・ＬＡＮで使用するプロトコルを示す図である。

【図６】ＴＣＰ／ＩＰ・ＬＡＮのパケット・フォーマットである。

【図７】ＴＣＰのヘッダフォーマットである。

【図８】本発明の一実施例のセッション確立手順のシーケンスチャートである。

【図９】本発明の一実施例のセッション切断手順のシーケンスチャートである。

【図１０】本発明の一実施例の鍵配送手順を示すシーケンスチャートである。

12

【図１１】本発明の一実施例の暗号ゲートウェイ装置の鍵配送センタからの鍵取得のシーケンスチャートである。

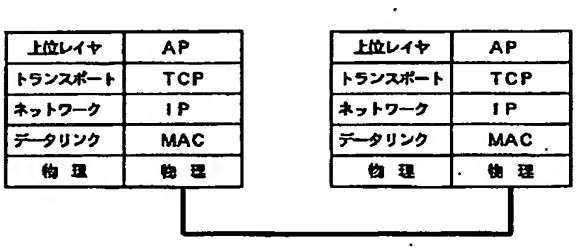
【図１２】従来の暗号通信システムの構成を示す。

【図１３】従来の暗号通信システムを説明するための図である。

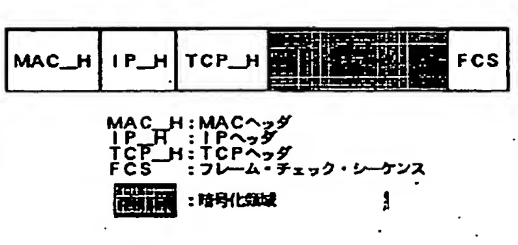
【符号の説明】

１　鍵配送センタ
２　ネットワーク
３　クライアント
４　暗号ゲートウェイ装置
５　サーバ
３１　セッション制御部
３２　セッション鍵配送部
３３　鍵管理部
３４　セッション鍵配送部
３５　暗号化／復号部
３６　送信／受信部
４１　セッション確立／切断のモニタ部
４２　セッション鍵配送部
４３　鍵管理部
４４　暗号同期確立部
４５　送信／受信部
４６　セッション識別部
４７　暗号化／復号部
１０１　鍵取得手段
１０２　クライアント鍵管理手段
１０３　クライアント同期確立手段
１０４　鍵配送手段
１０５　ゲートウェイ鍵管理手段
１０６　ゲートウェイ同期確立手段
１０７　第１の暗号化／復号手段
１０８　無効手段
１０９　破棄手段
１１０　第２の暗号化／復号手段

【図５】

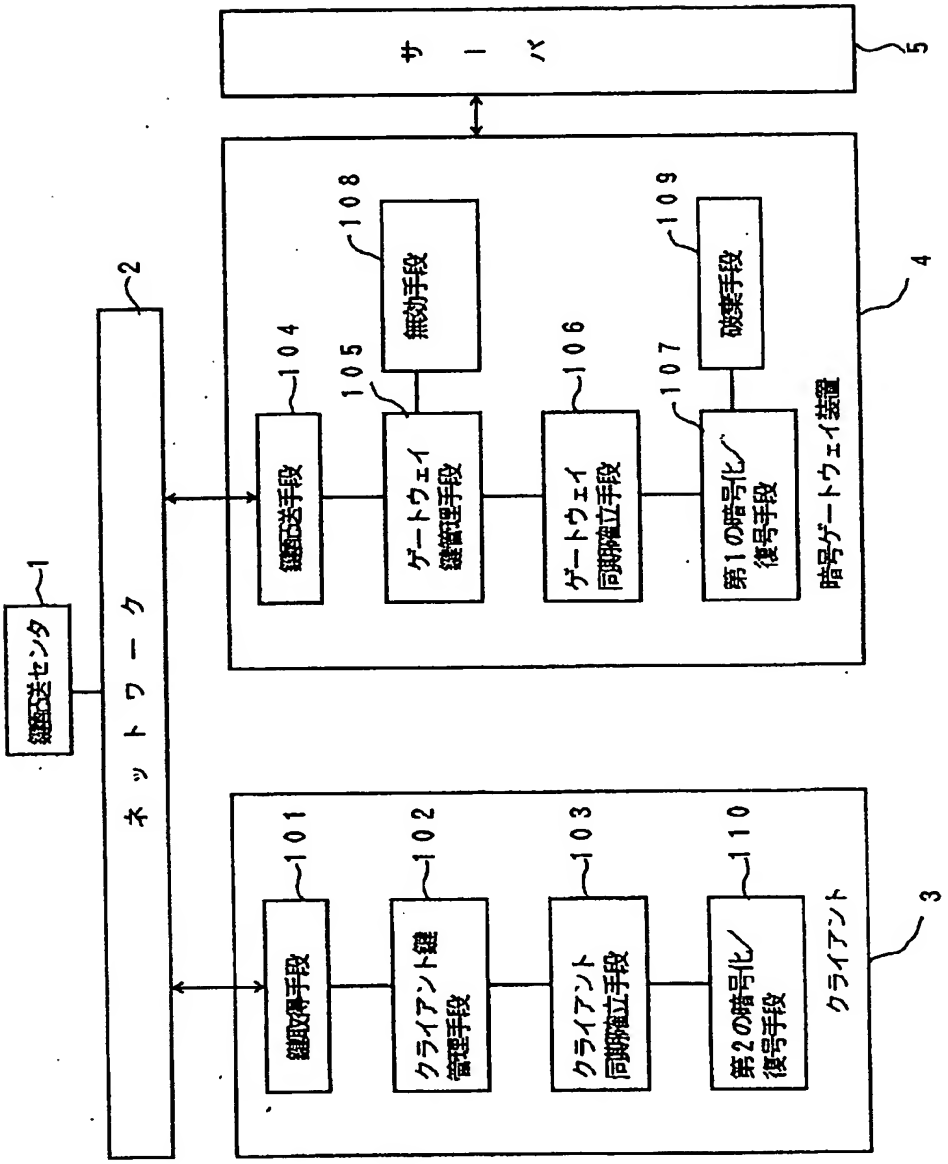


【図６】



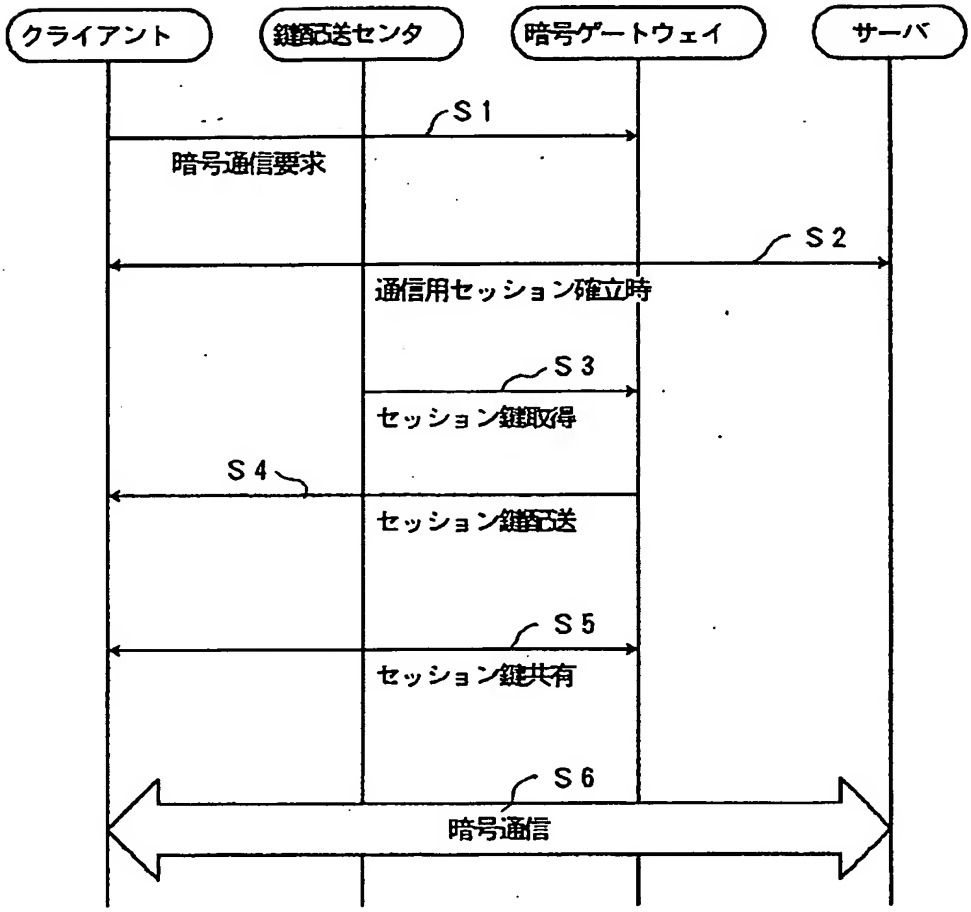
【図１】

本発明の原理構成図

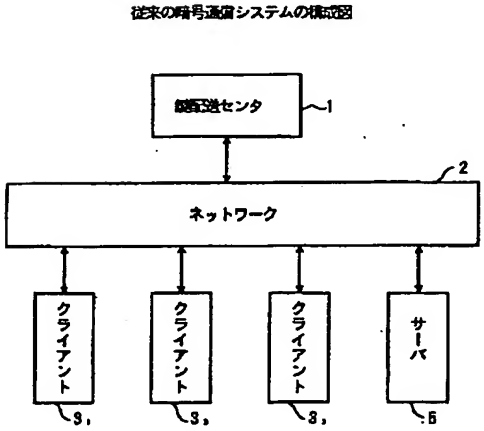


【図２】

本発明の概要のシーケンス

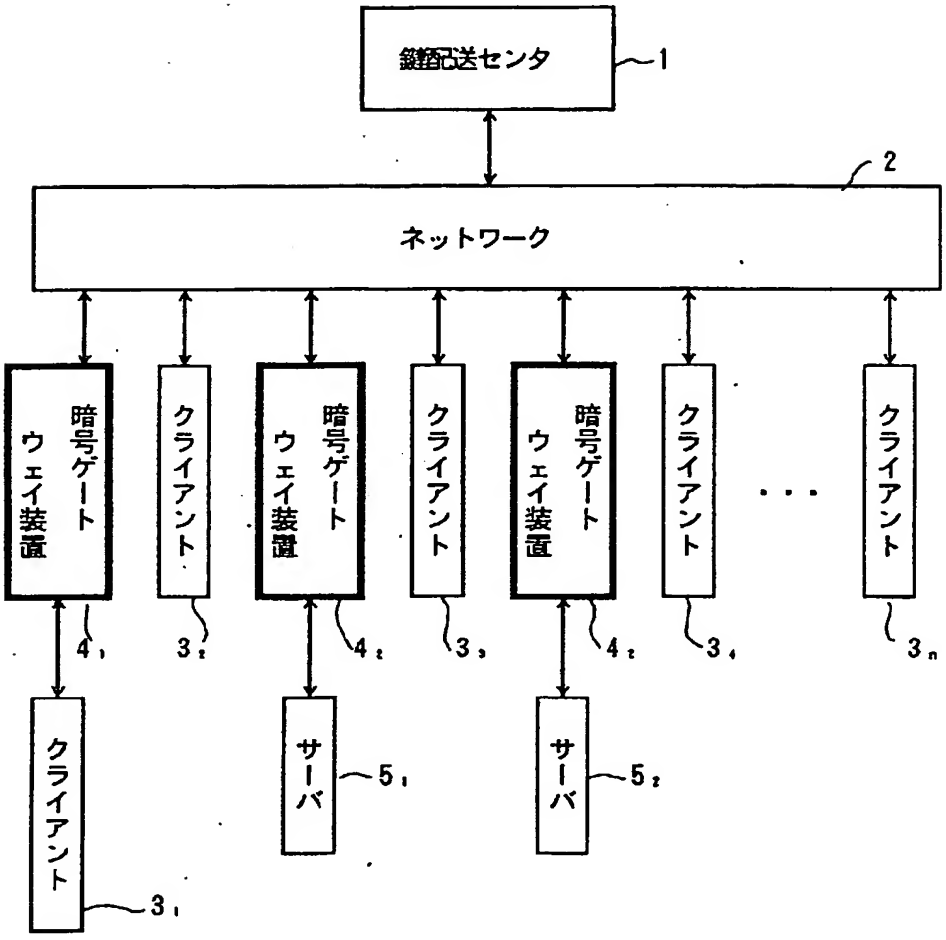


【図１２】



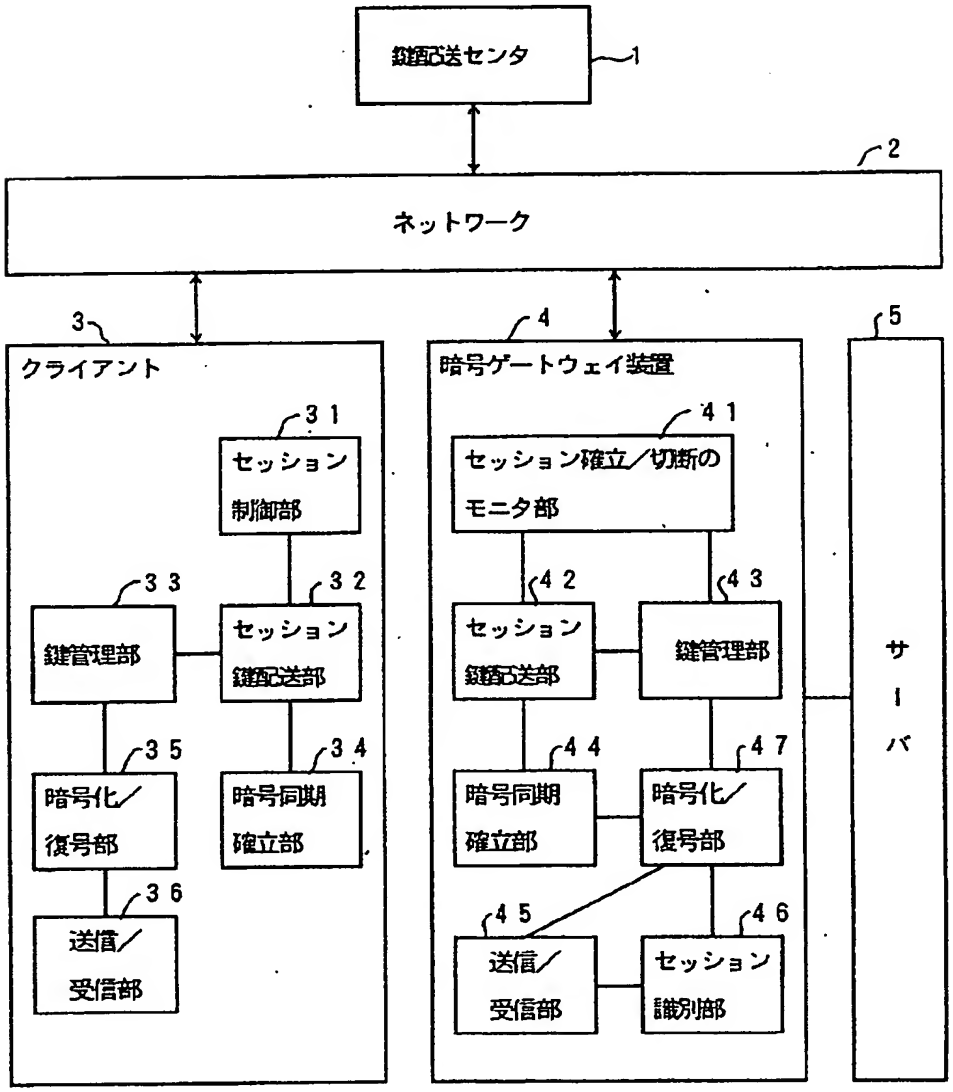
【図３】

本発明のシステム全体図



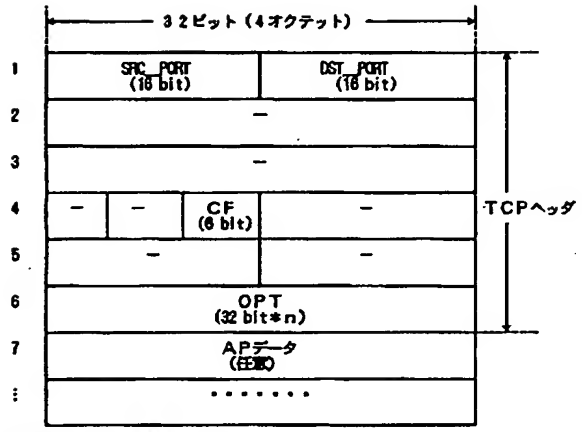
【図４】

本発明の一実施例のシステム構成図



【図７】

TCPヘッダのフォーマット

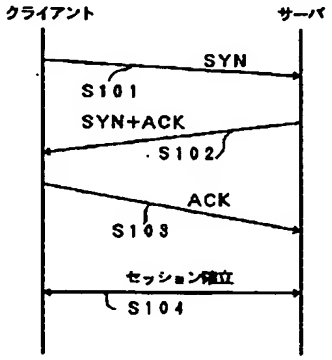


SRCPORT：ソース・ポート
DESTPORT：デスティネーション・ポート
CF：制御フラグ

SYN(Synchronize Flag)：セッションの確立
ACK(Acknowledgement Flag)：確認
FIN(Fin Flag)：セッションの切断
OPT：オプション

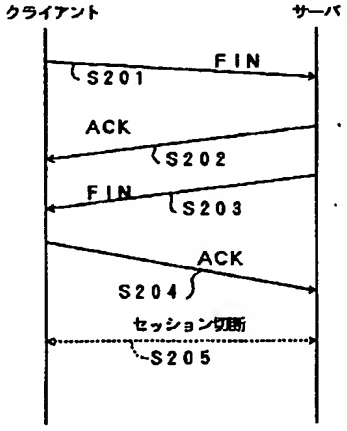
【図８】

本発明の一実施例のセッション確立手段のシーケンスチャート



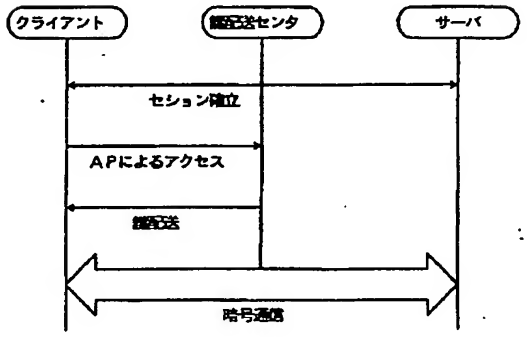
【図９】

本発明の一実施例のセッション切断手段のシーケンスチャート

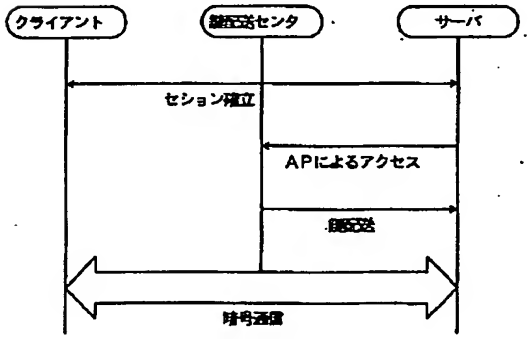


【図１３】

従来の暗号通信システムを説明するための図



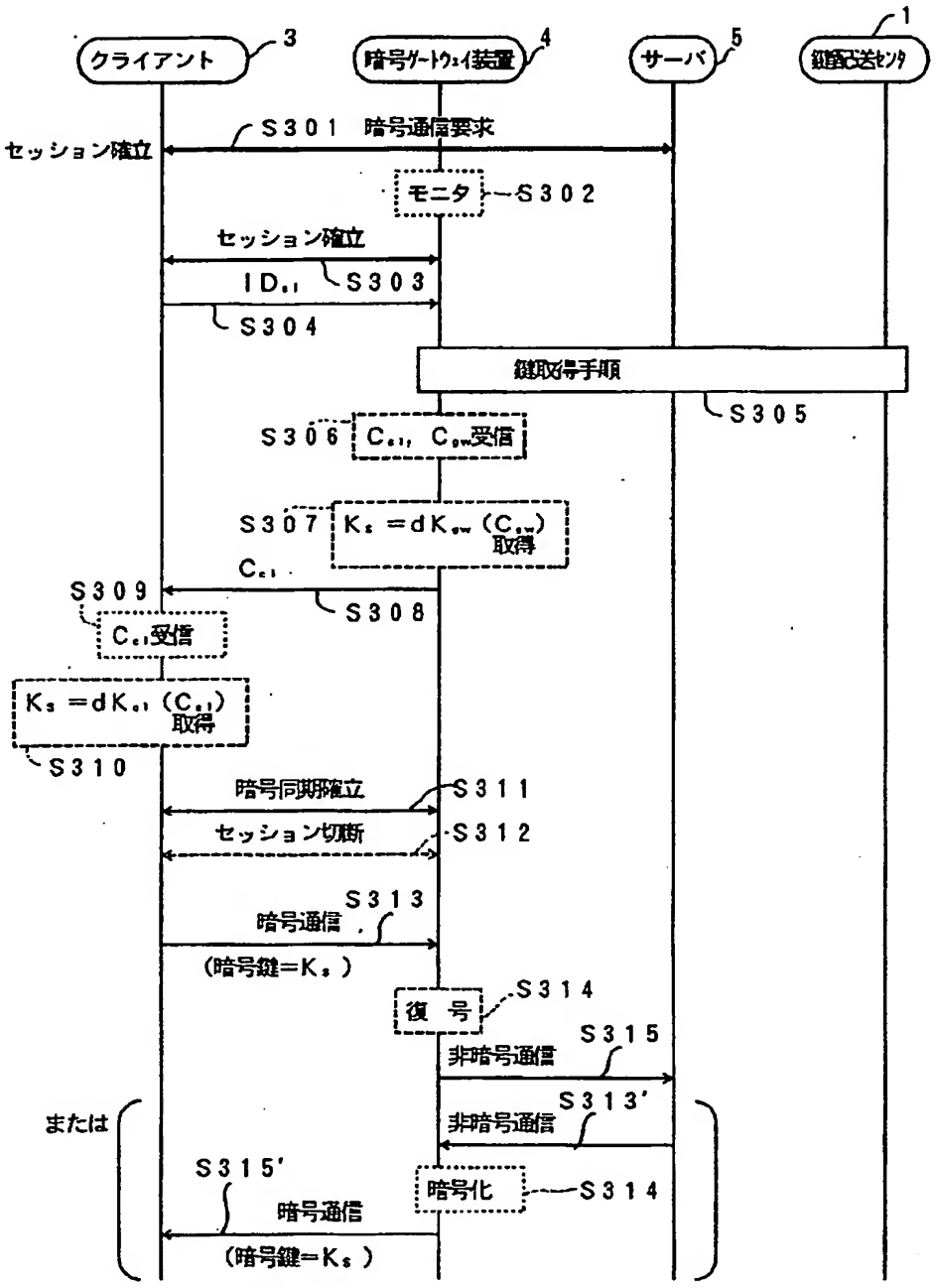
(A)



(B)

【図１０】

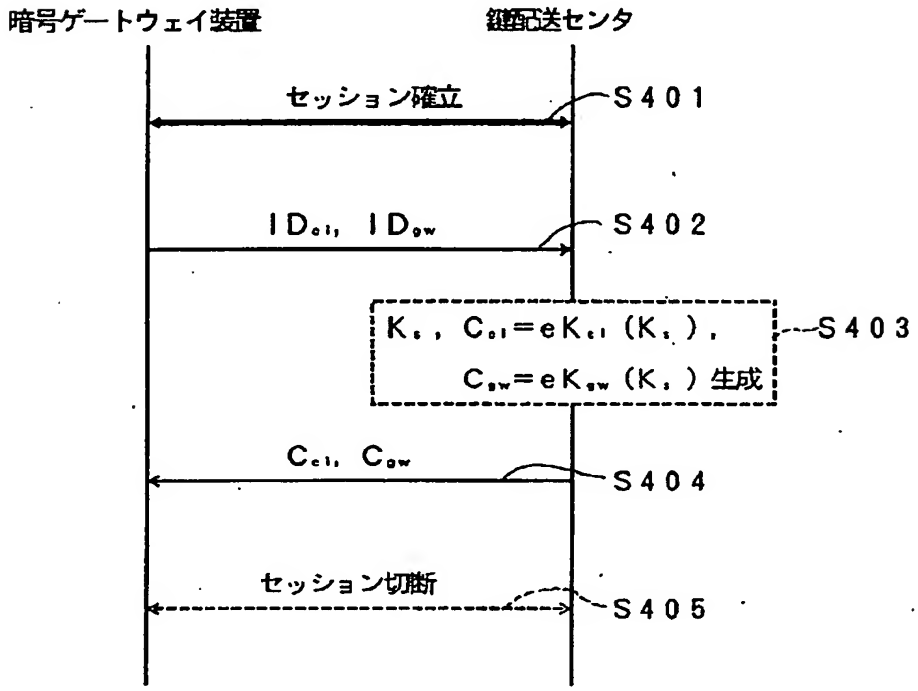
本発明の一実施例の鍵配送手段を示すシーケンスチャート



(注) Kₛ＝dK₀₁(C₀₁)：Kₛは、暗号文C₀₁を暗号鍵K₀₁で復号した結果である。

【図１１】

本発明の一実施例の暗号ゲートウェイ装置の鍵配送センタからの鍵取得のシーケンスチャート



（注）Cc1＝eKc1（Ks）：Cc1は平文Ksを暗号鍵Kc1で暗号化した結果である。

フロントページの続き

(56)参考文献　特開　昭63－274242（ＪＰ，Ａ）
特開　平４－179326（ＪＰ，Ａ）
特開　平７－107083（ＪＰ，Ａ）
山口利和，田中清人，田辺克弘，小柳津育郎，ＬＡＮの暗号通信における一方式，電子情報通信学会技術研究報告（ＯＦＳ93－32），日本，社団法人電子情報通信学会，1994年　１月21日，Ｖｏｌ．93，Ｎｏ．435，ｐ．13－18
山口利和，田中清人，田辺克弘，小柳津育郎，ＬＡＮ暗号通信方式の実装と評価，電子情報通信学会技術研究報告（ＯＦＳ93－38），日本，社団法人電子情報通信学会，1994年　３月11日，Ｖｏｌ．93，Ｎｏ．508，ｐ．７－12
山口利和，田中清人，田辺克弘，小柳津育郎，ＬＡＮセキュリティ通信技術－ＴＣＰレイヤにおける通信データの暗号化－，ＮＴＴ　Ｒ＆Ｄ，日本，社団法人電気通信協会，1995年　７月　８日，Ｖｏｌ．44，Ｎｏ．９，ｐｐ．653－660

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L　9/08
H04L　12/28